

IN THE DRAWINGS:

In Figure 8 of the drawings, the spelling of the word “problem” has been corrected. Also, in Figure 13 of the drawings the spelling of the words “provider”, “conversion” and “convert” has been corrected. Submitted concurrently herewith is a Letter to the Office Draftsperson submitting replacement drawing sheets for Figures 8 and 13 including the above identified corrections. Entry of these drawing corrections is respectfully requested.

REMARKS

The above amendments to the above-captioned application along with the following remarks are being submitted as a full and complete response to the Official Action dated April 20, 2005 (Paper No. 20050405). In view of the above amendments and the following remarks, the Examiner is respectfully requested to give due reconsideration to this application, to indicate the allowability of the claims, and to pass this case to issue.

Status of the Claims

Claims 2 through 8 are currently pending in the above-identified application. Claims 2 through 4 have been previously withdrawn from consideration. Also, Claim 1 has been cancelled without prejudice or disclaimer. Further, Claims 6 and 7 are being amended to correct formal errors, place the claims in better form and to more particularly point out and distinctly claim the subject invention. Entry of the amendments to Claims 6 and 7 is respectfully requested.

Additional Amendments

The Specification has been amended to correct formal errors and to better disclose and describe the features of the present invention. Entry of the amendments to the Specification is respectfully requested.

Also, Figures 8 and 13 of the drawings have been amended. In Figure 8 of the drawings, the spelling of the word "problem" has been corrected. Also, in Figure 13 of the drawings the spelling of the words "provider", "conversion" and "convert" has been corrected. Entry of the amendments to Figures 8 and 13 of the drawings is respectfully requested.

Formal Objections/Rejections

Figure 8 of the drawings was objected to as to the spelling of the word "problem". In response, Figure 8 has been amended and the replacement sheet for Figure 8 includes the corrected spelling of the word "problem". Therefore, withdrawal of the objection to Figure 8 of the drawings is respectfully requested.

Claims 6 and 7 were objected to in view of informalities. In response, Claims 6 and 7 have been amended and include amendments addressing these informalities. Therefore, withdrawal of the objection to Claims 6 and 7 is respectfully requested.

Claim 7 was rejected under 35 U.S.C. § 112, first paragraph, as allegedly failing to

comply with the enablement requirement by the including of the wording “notifying, from said server system, said client system of said client system”. In response, Claim 7 has been amended and includes amendments addressing this rejection under 35 U.S.C. § 112, first paragraph. Therefore, withdrawal of the rejection of Claim 7 under 35 U.S.C. § 112, first paragraph, is respectfully requested.

Prior Art Rejections

Claim 1 was rejected under 35 U.S.C. § 102(b) over Matsumoto et al., “Speeding up Secret Computations with Insecure Auxiliary Devices”, hereinafter Matsumoto. In response, Claim 1 has been cancelled without prejudice or disclaimer. Therefore withdrawal of the rejection of Claim 1 under 35 U.S.C. § 102(b) is respectfully requested.

Claims 5 through 8 were rejected under 35 U.S.C. § 103(a) over Matsumoto. This rejection is respectfully traversed.

Claims 6 and 7 were rejected under 35 U.S.C. § 103(a) over Matsumoto in view of U.S. Patent No. 5,974,400 to Kagami et al., hereinafter the Kagami ‘400 Patent. This rejection is respectfully traversed.

The above rejections of Claims 5 through 8 and Claims 6 and 7 under 35 U.S.C. § 103(a) will be considered collectively.

Independent Claims 5 and 8 are directed to a solving system, solving service processing methods and a program for solving an optimization problem by use of an outside server.

In this regard, the solving system of independent Claim 5 includes:

- a conversion matrix generation routine for generating a nonsingular matrix P having m rows and m columns and a permutation matrix Q having n rows and n columns by using the ciphering key input from the ciphering key input interface; and

- a problem conversion routine for converting the optimization problem into another optimization problem having a different equality constraint $(PAQ)y = Pb$, a different inequality constraint $y \geq 0$, and a different objective function $f(Qy)$, by using the nonsingular matrix P and the permutation matrix Q .

Also, in this regard, the solving service processing method of independent Claim 6 includes:

- sending a program from the server system to the client system in response to a service start request issued by the client system, the program making a computer

implement:

(1) a problem input function of accepting a user's input of an optimization problem represented by an equality constraint $Ax = b$ defined by a coefficient matrix A having m rows and n columns and an m -dimensional right hand side vector b , an inequality constraint $x \geq 0$, and an objective function $f(x)$ to be minimized;

(2) a ciphering key input function of accepting a ciphering key from the user;

(3) a conversion matrix generation function of generating a nonsingular matrix P having m rows and m columns and a permutation matrix Q having n rows and n columns by using the ciphering key input by the ciphering key input function;

(4) a problem conversion function of converting the optimization problem into another optimization problem having a different equality constraint $(PAQ)y = Pb$, a different inequality constraint $y \geq 0$, and a different objective function $f(Qy)$, by using the nonsingular matrix P and the permutation matrix Q ;

(5) a problem output function of outputting the converted optimization problem to send it to an external system;

(6) a solution input function of receiving a solution y of the converted problem from the external system;

(7) a reverse conversion function of conducting reverse conversion $x = Qy$ on the solution y by using the matrix Q generated by the function of (3) and thereby finding a solution x of the original problem; and

(8) a solution output function of outputting the reverse-converted solution x ; receiving, in the client system, the program;

implementing, in the client system, the functions of (1), (2), (3), (4) and (5) of the received program, thereby converting an optimization problem into a different problem, and sending the different problem to the server system;

finding, in the server system, a solution y of the received different problem;

sending the solution y from the server system to the client system; and

implementing, in the client system, the functions of (6), (7) and (8) of the program, and thereby obtaining a solution x of the original optimization problem.

Further, in this regard, the solving service processing method of independent Claim 7 includes:

sending, from the program providing system, a program to the client system, the

program making a computer implement:

(1) a problem input function of accepting a user's input of an optimization problem represented by an equality constraint $Ax = b$ defined by a coefficient matrix A having m rows and n columns and an m -dimensional right hand side vector b , an inequality constraint $x \geq 0$, and an objective function $f(x)$ to be minimized;

(2) a ciphering key input function of accepting a ciphering key from the user;

(3) a conversion matrix generation function of generating a nonsingular matrix P having m rows and m columns and a permutation matrix Q having n rows and n columns by using the ciphering key input by the ciphering key input function;

(4) a problem conversion function of converting the optimization problem into another optimization problem having a different equality constraint $(PAQ)y = Pb$, a different inequality constraint $y \geq 0$, and a different objective function $f(Qy)$, by using the nonsingular matrix P and the permutation matrix Q ;

(5) a problem output function of outputting the converted optimization problem to send it to an external system;

(6) a solution input function of receiving a solution y of the converted problem from the external system;

(7) a reverse conversion function of conducting reverse conversion $x = Qy$ on the solution y by using the matrix Q generated by the function of (3) and thereby finding a solution x of the original problem; and

(8) a solution output function of outputting the reverse-converted solution x ; receiving, in the client system, the program;

implementing, in the client system, the functions of (1), (2), (3), (4) and (5) of the received program, thereby converting an optimization problem into a different problem, and sending the different problem to the server system;

finding, in the server system, a solution y of the received different problem;

sending the solution y from the server system to the client system; and

implementing, in the client system, the functions of (6), (7) and (8) of the program, and thereby obtaining a solution x of the original optimization problem.

Additionally, independent Claim 8 recites a program for making a computer implement:

a problem input function of accepting an input of an optimization problem

represented by an equality constraint $Ax = b$ defined by a coefficient matrix A having m rows and n columns and an m -dimensional right hand side vector b , an inequality constraint $x \geq 0$, and an objective function $f(x)$ to be minimized;

a ciphering key input function of accepting a ciphering key;

a conversion matrix generation function of generating a nonsingular matrix P having m rows and m columns and a permutation matrix Q having n rows and n columns by using the ciphering key input by the ciphering key input function;

a problem conversion function of converting the optimization problem into another optimization problem having a different equality constraint $(PAQ)y = Pb$, a different inequality constraint $y \geq 0$, and a different objective function $f(Qy)$, by using the nonsingular matrix P and the permutation matrix Q ;

a problem output function of outputting the converted optimization problem;

a solution input function of receiving a solution y of the converted problem;

a reverse conversion function of conducting reverse conversion $x = Qy$ on the solution y by using the matrix Q generated by the conversion matrix generation function and thereby finding a solution x of the original problem; and

a solution output function of outputting the reverse-converted solution x .

In contrast, Matsumoto teaches that a small device or a smart card executes computation using computing power of auxiliary devices and that the small device has a secret computation (See page 497, paragraphs 1-3 of Matsumoto). Further, Matsumoto teaches the protocol MM and the speeding up the RSA transformations with the RSA cryptosystem (See pages 500-502 of Matsumoto)

Also, the Kagami '400 Patent teaches to send a service identifier to the server to receive therefrom the program for the service. (See Abstract of the Kagami' 400 Patent)

In view of the foregoing, it is respectfully submitted that Matsumoto and the Kagami '400 Patent do not teach or disclose the above identified features of a solving system, solving service processing methods and a program for solving an optimization problem by use of an outside server, as respectively recited in independent Claims 5 through 8.

Therefore, in view of the above discussion, it is respectfully submitted that independent Claims 5 through 8 are not anticipated by Matsumoto, and are not obvious over Matsumoto in view of the Kagami '400 Patent.

Withdrawal of the rejections of Claim 1 under 35 U.S.C. § 102(b) and Claims 5

through 8 under 35 U.S.C. § 103(a) is respectfully requested.

Reconsideration and allowance of Claims 5 through 8, and consideration of withdrawn Claims 2 through 4, are respectfully requested.

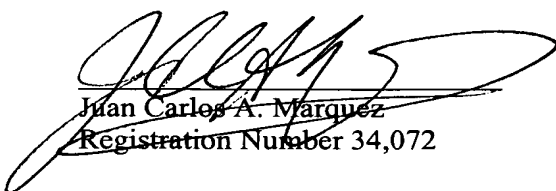
Conclusion

In view of all the above, Applicants respectfully submit that certain clear and distinct differences as discussed exist between the present invention as now claimed and the prior art references upon which the rejections in the Office Action rely. These differences are more than sufficient that the present invention as now claimed would not have been anticipated nor rendered obvious given the prior art. Rather, the present invention as a whole is distinguishable, and thereby allowable over the prior art.

Favorable reconsideration of this application as amended is respectfully solicited. Should there be any outstanding issues requiring discussion that would further the prosecution and allowance of the above-captioned application, the Examiner is invited to contact the Applicants' undersigned representative at the address and telephone number indicated below.

Respectfully submitted,

Stanley P. Fisher
Registration Number 24,344


Juan Carlos A. Marquez
Registration Number 34,072

REED SMITH LLP
3110 Fairview Park Drive, Suite 1400
Falls Church, Virginia 22042
(703) 641-4200

October 20, 2005

SPF/JCM/JB